WUTC DOCKET: 181051
EXHIBIT: JHJ-4
ADMIT ☑ W/D ☐ REJECT ☐

**Exh. JHJ-4**
**Docket UT-181051**
**Witness: Jacque Hawkins-Jones**

**BEFORE THE WASHINGTON**
**UTILITIES AND TRANSPORTATION COMMISSION**

| | |
|---|---|
| **WASHINGTON UTILITIES AND TRANSPORTATION COMMISSION,**<br><br>**Complainant,**<br><br>**v.**<br><br>**CENTURYLINK COMMUNICATIONS, LLC.,**<br><br>**Respondent.** | **DOCKET UT-181051** |

**EXHIBIT TO**
**TESTIMONY OF**

**JACQUE HAWKINS-JONES**

**STAFF OF**
**WASHINGTON UTILITIES AND**
**TRANSPORTATION COMMISSION**

***Narrative of Federal Communication Commission Investigation Report***

**December 15, 2021**

# Appendix C

# December 27, 2018 CenturyLink Network Outage Report

A Report of the Public Safety and Homeland Security Bureau
Federal Communications Commission
August 19, 2019

**TABLE OF CONTENTS**

## I. INTRODUCTION

1. In the early morning of December 27, 2018, CenturyLink experienced a nationwide outage on its fiber network that lasted for almost 37 hours. This outage was caused by an equipment failure catastrophically exacerbated by a network configuration error. It affected communications service providers, business customers, and consumers who directly or indirectly relied upon CenturyLink's transport services, which route communications traffic from various providers to locations across the country, resulting in extensive disruptions to phone service, including 911 calling. The effects included dropped calls, disconnected 911 call centers (known as "Public Safety Answering Points"), and fast-busy signals for people who called 911. As many as 22 million customers across 39 states were affected by the outage, including approximately 17 million customers across 29 states who lacked reliable access to 911. Indeed, at least 886 calls to 911 were not delivered.[1] Fortunately, based on discussions with affected service providers and public safety officials from affected states, as well as a review of media reports, the Public Safety and Homeland Security Bureau (Bureau) is not aware of any harm to life or property resulting from the outage.

2. The Bureau investigated the incident, its effects, and the recovery. As part of its investigation, Bureau staff reviewed and analyzed outage reports filed in the Network Outage Reporting System (NORS) and held meetings with relevant stakeholders, including service providers and public safety entities.[2] This report presents the Bureau's findings and recommendations. This outage provides the Commission and stakeholders with the opportunity to learn valuable lessons about network reliability and the implementation of industry-accepted best practices. For example, this outage demonstrates the importance of either turning off or otherwise disabling unused system features to prevent unintentional and unmonitored use of those features that can result in negative, unintended consequences. In addition, network administrators should have secondary network monitoring procedures in place for when primary network monitoring procedures are inoperable or insufficient.

## II. BACKGROUND

3. One of the Commission's primary objectives is to "make available, so far as possible, to all people of the United States . . . a . . . wire and radio communication service . . . for the purpose of promoting safety of life and property."[3] In furtherance of this objective, the Commission has taken measures to promote the reliable and continued availability of 911 telecommunications service and

---

[1] This total includes eleven calls to 911 handled by CenturyLink, 75 calls to 911 handled by West Safety Services, and approximately 800 calls to 911 handled by General Dynamics Information Technology.

[2] NORS is the Commission's web-based filing system through which communications providers covered by the Part 4 outage reporting rules must submit reports to the Commission. These reports are presumed confidential to protect sensitive and proprietary information about communications networks. *See* 47 CFR § 4.2.

[3] 47 U.S.C. § 151. Congress has repeatedly and specifically endorsed a role for the Commission in the nationwide implementation of advanced 911 capabilities. *See* Wireless Communications and Public Safety Act of 1999, PL 106–81, 113 Stat 1286 §§ 3(a), (b) (1999) (codified at 47 U.S.C. § 251(e)(3), 47 U.S.C. § 615) (directing the Commission to "designate 911 as the universal emergency telephone number within the United States for reporting an emergency to appropriate authorities and requesting assistance" and to "encourage and support efforts by States to deploy comprehensive end-to-end emergency communications infrastructure and programs, based on coordinated statewide plans, including seamless, ubiquitous, reliable wireless telecommunications networks and enhanced wireless 911 service."); *see also* New and Emerging Technologies 911 Improvement Act of 2008 (NET 911 Act), PL 110–283, 122 Stat 2620 (2008) (codified at 47 U.S.C. § 615a-1(a), (c)(1)(B)) (requiring "each IP-enabled voice service provider to provide 9-1-1 service and enhanced 9-1-1 service to its subscribers in accordance with the requirements of the Federal Communications Commission"); Twenty–First Century Communications and Video Accessibility Act of 2010, PL 111-260, 124 Stat 2751 § 106(g) (2010) (CVAA) (codified at 47 U.S.C. § 615c(g)).

telephone service generally.[4] With specific regard to 911 services, the Commission requires telecommunications carriers and commercial mobile radio service providers to transmit 911 calls to a Public Safety Answering Point (PSAP) (or, in rare cases, to another appropriate local emergency authority).[5]

4. The Commission stays abreast of major disruptions to our nation's communications infrastructure through outage reports filed by communications providers in the wake of major disruptions to their networks. As part of this reporting framework, Commission rules require service providers to report communication disruptions affecting major transport facilities.[6] The Commission uses the term "major transport facility" to describe communications infrastructure components that have significant traffic-carrying capacity.[7] Under the Commission's network outage reporting rules, the minimum threshold capacity for outage reporting purposes is defined as an OC3 circuit or its equivalent.[8] An OC3 circuit has the capacity to transmit data at a rate of 155.52 Mbit/s using fiber optics, and is often used to transmit large amounts of data, including multiple telephone calls simultaneously. A major transport provider is required to file an outage report when an OC3 circuit (or its equivalent) that the provider owns, operates, leases, or otherwise utilizes experiences a communication disruption that lasts for at least 30 minutes and meets the 667 OC3 minute threshold.[9]

5. The Commission has adopted PSAP outage notification requirements where service providers discover outages that could affect the delivery of 911 calls.[10] In addition to these network outage reporting rules, the Commission's 911 reliability rules require certain providers – known as originating service providers – to convey all available and potentially useful information to the PSAP during a 911 outage to help mitigate the effects of the outage on those who might call that PSAP.[11] Originating service providers include cable communications providers, satellite operators, wireless service providers, and wireline communications providers – entities that offer the ability "to originate 911 calls."[12] The Commission also requires covered 911 service providers – service providers that offer core

---

[4] *See Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, CC Docket No. 94-102, RM-8143, Memorandum Opinion and Order, 12 FCC Rcd 22665, 22744 (1997); *Transition from TTY to Real-Time Text Technology; Petition for Rulemaking to Update the Commission's Rules for Access to Support the Transition from TTY to Real-Time Text Technology and Petition for Waiver of the Rules Requiring Support for TTY Technology*, CG Docket No. 16-145, GN Docket No. 15-178, Report and Order and Further Notice of Proposed Rulemaking, 31 FCC Rcd 13568 (2016) (applying an analogous requirement to common carriers); *see also* 47 CFR § 20.18(b); 47 CFR § 64.3001.

[5] 47 CFR §§ 20.18, 64.3001, 64.3002.

[6] *See New Part 4 of the Commission's Rules Concerning Disruptions to Communications*, ET Docket No. 04-35, Report and Order and Further Notice of Proposed Rulemaking, 19 FCC Rcd 16830, 16895-902, paras. 127-143 (2004).

[7] *See, e.g.*, *New Part 4 of the Commission's Rules Concerning Disruptions to Communications*, ET Docket 04-35, Order Granting Partial Stay, 19 FCC Rcd 25039, 25042, para. 4 (2004).

[8] 47 CFR § 4.7(d).

[9] *2016 Part 4 Order*, 31 FCC Rcd at 5826, para. 17; *see also* 47 CFR § 4.7(d) (defining the OC3-based metric as OC3 minutes, "the mathematical result of multiplying the duration of an outage, expressed in minutes, by the number of previously operating OC3 circuits or their equivalents that were affected by the outage").

[10] *See New Part 4 of the Commission's Rules Concerning Disruptions to Communications*, ET Docket No. 04-35, Report and Order and Further Notice of Proposed Rulemaking, 19 FCC Rcd 16830 (2004) (*2004 Part 4 Report and Order*); 47 CFR § 4.9.

[11] *See New Part 4 of the Commission's Rules Concerning Disruptions to Communications*, ET Docket No. 04-35, Report and Order and Further Notice of Proposed Rulemaking, 19 FCC Rcd 16830 (2004); 47 CFR § 4.9.

[12] 47 CFR § 12.4(a)(4)(ii)(B) (defining an originating service provider); 47 CFR §§ 4.9(a), (c), (e), (f) (detailing parallel PSAP notification requirements for cable, satellite, wireless and wireline service providers); *see also*

911 capabilities or deliver 911 calls and associated number or location information to the appropriate PSAP – to notify 911 special facilities of outages that potentially affect them within 30 minutes of discovering an outage and to update PSAPs within two hours of initial contact to communicate information about the nature of the outage, its best-known cause, its geographic scope, and the estimated time for repairs.[13]

6. Covered 911 service providers are required to take reasonable measures to provide reliable 911 service in three specific respects: circuit diversity, central office backup power, and diverse network monitoring.[14] They must also "certify annually whether they have, within the past year, audited the physical diversity of critical 911 circuits or equivalent data paths to each PSAP they serve, tagged those circuits to minimize the risk that they will be reconfigured at some future date, and eliminated all single points of failure."[15] In the alternative, covered 911 service providers may describe "reasonably sufficient alternative measures they have taken to mitigate the risks associated with the lack of physical diversity."[16] Similar obligations apply to their network monitoring capabilities.[17]

## III. INCIDENT AND RESPONSE

### A. Architecture of CenturyLink's Network

7. CenturyLink operates six separately managed long-haul networks that provide transport for telecommunications traffic across the country. The CenturyLink network affected by this outage provides high-speed data transport over optical fiber. It is used by individual and enterprise customers for myriad purposes, including 911 services, Voice over Internet Protocol (VoIP), local and long-distance voice, ethernet, Internet Protocol (IP) backbone, consumer Digital Subscriber Line (DSL) and other services.

8. In the affected network, network traffic transits across nodes, where data enters and exits the network. At the time of the outage, the affected network used nodes supplied by Infinera Intelligent Transport Networks (Infinera).[18] Each node provides optical fiber switching, a process that ensures that network traffic is directed towards the intended network path, between networks components called line modules. Line modules provide the connection points between nodes across the country. Internal to each node, a component called a switching module transfers packets from inbound line modules to outbound line modules. The switching module directs traffic that arrives on a particular port and stream of an

(Continued from previous page)
*Improving 911 Reliability; Reliability and Continuity of Communications Networks, Including Broadband Technologies*, PS Docket Nos. 13-75, 11-60, Report and Order, 28 FCC Rcd 17476, 17488-89, para. 36 (2013) (*911 Reliability Order*).

[13] 47 CFR § 12.4(a)(4) (defining a covered 911 service provider). *Compare* 47 CFR § 4.9(h) (requiring covered 911 service providers to notify affected PSAPs "no later than 30 minutes from discovering the outage) *with* 47 CFR § 4.9(e) (requiring originating service providers to notify affected PSAPs "as soon as possible"). The Commission's PSAP notification requirements for covered 911 service providers are generally more specific than those that apply to originating service providers.

[14] 47 CFR § 12.4(b).

[15] *911 Reliability Order*, 28 FCC Rcd at 17503, para. 80; *see also* 47 CFR § 12.4(c)(1). Diversity audits check for "single points of failure" in network configurations, while tagging ensures that changes to critical 911 assets cannot be made without rigorous review.

[16] *911 Reliability Order*, 28 FCC Rcd at 17503, para. 80; 47 CFR § 12.4(b). This 2013 proceeding deferred for future consideration whether network reliability requirements should be extended to originating service providers. *See 911 Reliability Order*, 28 FCC Rcd at 17528-29, para. 147.

[17] 47 CFR § 12.4(c)(3).

[18] Infinera provides equipment and professional services to CenturyLink.

inbound line module to the correct port on the correct outbound line module. This report refers to this successful traffic direction as "synchronization." Correct synchronization ensures the line modules internal to the node are mapped correctly. Lack of synchronization would cause network data to drop or be corrupted as either an inbound line module would send traffic to the wrong outbound line module, or an outbound line module would attempt to receive traffic from the wrong inbound line module. Figure 1 conceptually shows how the Infinera nodes, line modules, and switching modules act together to send and receive network traffic from other nodes across the country.

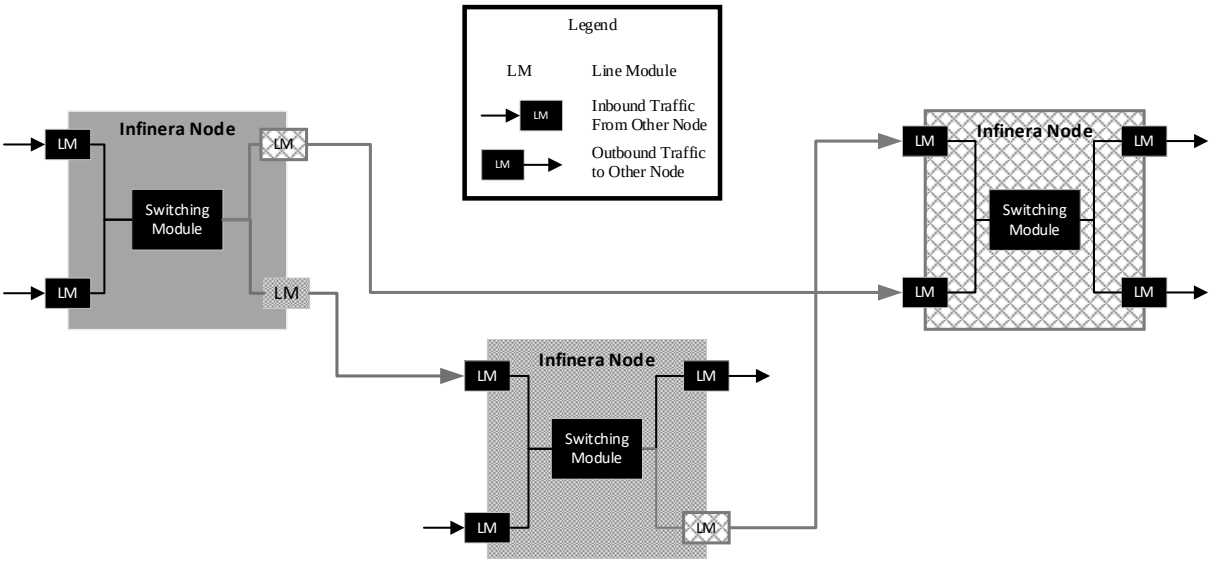


*Figure 1: Conceptual Infinera Node Interconnection Diagram*

9. The nodes in the affected network possess a proprietary internode management channel. This proprietary management channel is designed to allow for very fast, automatic rerouting of traffic to avoid a loss of traffic during a failure in the network. It does this by enabling line modules to send packets directly to other connected nodes without receiving network management instructions about how to route traffic.[19] To prevent management instructions from being sent to other nodes, the proprietary management channel has a filter that prevents packets that are 64 bytes or fewer from using the channel.[20] As the supplier of these nodes, Infinera provides its customers – including CenturyLink in this case – with the proprietary management channel enabled by default. CenturyLink was aware of the channel but neither configured nor used it.

## B. Root Cause and Event Summary

10. In the early morning of December 27, 2018, a switching module in CenturyLink's Denver, Colorado node spontaneously generated four malformed management packets.[21] Malformed packets are packets that, while not rare, are not typically generated on a network and are usually discarded

[19] In the Bureau's discussions with Infinera, Infinera used the term "packet" to describe what some experts refer to as Ethernet frames that are sent between nodes. For the sake of simplicity, this report uses the term "packet."

[20] Network management packets in the affected nodes are exactly 64 bytes in size and are intended to be discarded by the filter. Invalid packet fragments, which are likely to be less than 64 bytes in size, are also intended to be discarded.

[21] CenturyLink does not know the exact time when the switching module generated the malformed packets. However, CenturyLink asserts that its post-outage analysis shows that symptoms of a major network event were present at 3:40 a.m.

immediately due to characteristics that indicate that the packets are invalid. In this instance, the malformed packets included fragments of valid network management packets that are typically generated. Each malformed packet shared four attributes that contributed to the outage: 1) a broadcast destination address, meaning that the packet was directed to be sent to all connected devices; 2) a valid header and valid checksum; 3) no expiration time, meaning that the packet would not be dropped for being created too long ago; and 4) a size larger than 64 bytes. CenturyLink and Infinera state that, despite an internal investigation, they do not know how or why the malformed packets were generated.

11. The switching module that generated the malformed packets sent them as network management instructions to a line module. Figure 2 illustrates how the malformed packets then flowed through the network.[22] The packets were examined through a sequential series of conditions that produced either a "yes" or a "no" response. As shown in Figure 2, the malformed packets were able to pass each condition without being discarded. Because the packets were larger than 64 bytes, they were not stopped by the filter. Finally, while not shown, each malformed packet also passed the checksum condition, which is a test to determine if any errors occurred during the transmission of the packet, such as the changing of one or more bits in the message or if the message was randomly formed. As a result, the packets were transmitted along the enabled and unconfigured proprietary management channel.[23] The arriving malformed packets passed each condition at the nodes at which they arrived.

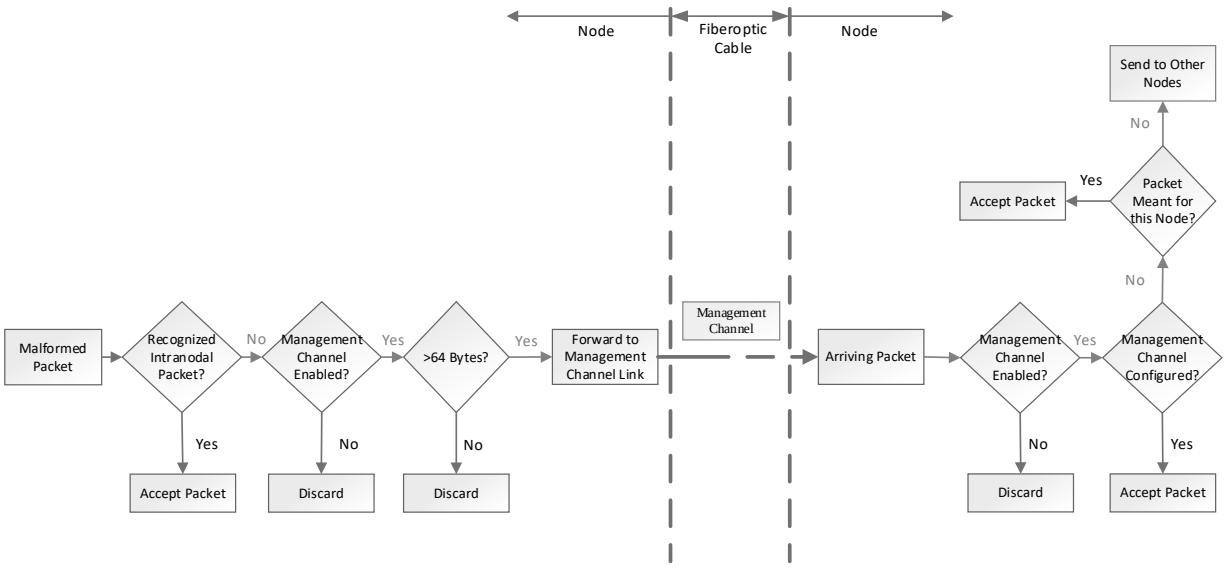


*Figure 2: Malformed Packet Distribution Flow Chart*

12. Due to the packets' broadcast destination address, the malformed network management packets were delivered to all connected nodes. Consequently, each subsequent node receiving the packet retransmitted the packet to all its connected nodes, including the node where the malformed packets originated. Each connected node continued to retransmit the malformed packets across the proprietary management channel to each node with which it connected because the packets appeared valid and did not have an expiration time. This process repeated indefinitely.

13. The exponentially increasing transmittal of malformed packets resulted in a never-ending feedback loop that consumed processing power in the affected nodes, which in turn disrupted the ability of the nodes to maintain internal synchronization. Specifically, instructions to output line modules would

[22] Figure 2 is intended to be illustrative of the conditions that are implicated in this outage. It is not intended to be representative of all of the conditions on this path, nor their actual order.

[23] In discussions with Bureau staff, Infinera used the terms 'unlocked' and 'locked' to describe the status of the channel. In the interest of clarity, this report instead uses the terms 'enabled' and 'disabled.'

lose synchronization when instructions were sent to a pair of line modules, but only one line module actually received the message. Without this internal synchronization, the nodes' capacity to route and transmit data failed. As these nodes failed, the result was multiple outages across CenturyLink's network.

### C. CenturyLink and Infinera Recovery and Restoration

14. CenturyLink first became aware that it was experiencing a major network incident upon receiving an inquiry from a customer near New Orleans, Louisiana at 3:56 a.m. on December 27, 2018.[24] While troubleshooting this customer complaint, multiple alarms indicated an issue with Infinera control modules. CenturyLink determined that the outage was widespread and began investigating. CenturyLink's network administrators were unable to connect to nodes remotely to locate and diagnose the outage or take corrective action because the nodes were overloaded.

15. At 4:25 a.m., CenturyLink network administrators in New Orleans engaged other CenturyLink administrators in San Antonio, Texas, as well as Infinera. By mid-morning on December 27, CenturyLink dispatched network engineers to Omaha, Nebraska and Kansas City, Missouri to log in to affected nodes directly. Network engineers in Kansas City found an address in a captured malformed packet indicating the malformed packets originated in the Denver, Colorado node. At 9:02 p.m. on December 27, CenturyLink network engineers identified and removed the module that had generated the malformed packets. The outage, however, did not immediately end; the malformed packets continued to replicate and transit the network, generating more packets as they echoed from node to node.

16. At 12:09 a.m. on December 28, a CenturyLink network engineer began instructing nodes to no longer acknowledge the malformed packets. CenturyLink network engineers also disabled the proprietary management channel, preventing it from further transmitting the malformed packets. CenturyLink and Infinera worked together to realign paired line modules to communicate through the same switching modules to ensure fiber optic synchronization and stability. By 5:07 a.m., CenturyLink and Infinera had returned much of the network to normal function. CenturyLink restored visibility into the network at 11:30 a.m. on December 28, meaning that all nodes became reachable via remote access. By 11:36 p.m., network engineers had restored all nodes in the affected network, though some customers experienced residual effects of the outage as CenturyLink continued to reset affected line modules and replace line modules that failed to reset.[25] On December 29, 2018, at 12:01 p.m., CenturyLink determined that the backbone network had stabilized.

## IV. IMPACT

### A. Impact on CenturyLink's Network

17. The event caused a nationwide voice, IP, and transport outage on CenturyLink's fiber network. CenturyLink estimates that 12,100,108 calls were blocked or degraded due to the incident. Where long-distance voice callers experienced call quality issues, some customers received a fast-busy signal, some received an error message, and some just had a terrible connection with garbled words. The outage also affected communications of state government entities: for example, in Idaho, the CenturyLink outage caused the temporary shutdown of phone services at both the Idaho Department of Correction and the state's Department of Education.[26] Four states, Illinois, Kansas, Minnesota, and

[24] All times mentioned in this report are Eastern Standard Time (EST).

[25] While the nodes had been restored, other services that had been negatively affected did not automatically come back online, necessitating further restoration work by CenturyLink and its vendors. For example, CenturyLink's own cloud services remained unavailable for over 20 hours after the network was restored.

[26] Ruth Brown & Michael Katz, *Widespread CenturyLink outage shuts down phone services at Idaho prisons, education dept.*, Idaho Statesman (Dec. 27, 2018), https://www.idahostatesman.com/news/local/article223619505.html.

Missouri, experienced network isolation for 36 hours, meaning services that relied on access to other parts of the network were disrupted. Fourteen other states, primarily in the western region of the country, experienced network congestion that may have affected service.[27] CenturyLink's IP backbone, which carries VoIP, IP, ethernet, and other services, was also affected. Approximately 250,000 CenturyLink IP service customers were affected or potentially affected by the outage, including approximately 4,000 enterprise customers in Idaho, Louisiana, Montana, Texas, and Wyoming. In addition, approximately 1.1 million CenturyLink DSL customers lost service during portions of the event, with the most significant effects occurring in Idaho, New Mexico, Oregon, and Utah. Another 2.6 million customers may have experienced degraded service. The effect on transport facilities was large: facilities with a capacity of approximately 300,000 OC3s were affected.[28] As described below, this event had rippling effects on other service providers that use the affected long-haul transport network, including service providers that provide 911 service.

## B. Impact on 911 Calls Handled by CenturyLink

18. The outage also affected 911 calls handled by CenturyLink. CenturyLink states that it timely notified the PSAPs that it serves and that it was in contact with the PSAPs it serves as a covered 911 service provider throughout the outage. During the outage, CenturyLink failed to deliver eleven 911 calls that had been forwarded to secondary Public Safety Answer Points (PSAPs) that it serves as a covered 911 service provider.[29] CenturyLink also failed to deliver automatic location information (ALI), which provides the PSAP with the caller's location, to fifteen PSAPs that CenturyLink serves as a covered 911 service provider in Arizona, Idaho, Montana, Utah, and Wyoming.[30]

## C. Impact on Other Service Providers

### 1. TeleCommunication Systems, Inc.

19. TeleCommunication Systems, Inc. (TeleCommunication Systems) is a wholly-owned subsidiary of Comtech Telecommunications Corp. that provides 911 service to originating service providers and PSAPs.[31] TeleCommunication Systems relies on the affected CenturyLink network for transport in processing some 911 calls. At 3:48 a.m. on December 27, 2018, CenturyLink's outage affected TeleCommunication Systems' processing of 911 calls from callers in Washington, north central Texas, and Tier 3 wireless service providers.[32] TeleCommunication Systems experienced multiple impairments to circuits provided by CenturyLink, which resulted in loss of circuit redundancy at various times over a combined duration of 49 hours and 32 minutes. This affected the routing of 911 calls to

[27] Network congestion can cause a range of impacts to customers' telephone service, from no effect to marginally degraded voice service to blocked calls.

[28] We note that although CenturyLink reported 52,286 OC3-equivalent capacity was affected, total transport capacity based on circuit outages appears to be closer to ~300,000 OC3s.

[29] A primary PSAP is the initial PSAP that the 911 call is routed to for answering. A secondary PSAP is a backup for the primary PSAP in case the 911 call cannot be routed to the primary PSAP or the 911 call cannot be answered by the primary PSAP. The precise roles of secondary PSAPs may vary depending on how 911 services are organized at the state or local level.

[30] This report describes the effects of the outage on 911 service that service providers and PSAPs reported to the Bureau during its investigation. While some entities provided a detailed description of effects to 911 services, such as the number of failed 911 calls, other entities did not have access to detailed information or did not report that information to the Bureau.

[31] TeleCommunication Systems relies on the CenturyLink transport network to carry 911 calls to PSAPs.

[32] A Tier 3 wireless carrier is a wireless provider that does not own the network upon which it operates.

TeleCommunication Systems' network by its Signaling System 7 (SS7) signaling provider.[33] According to TeleCommunication Systems, once it determined that it was experiencing issues with 911 calls, it notified affected PSAPs.

20. TeleCommunication Systems' networks that connect originating service providers with PSAPs in Washington and north central Texas were fully operational and able to receive calls from CenturyLink throughout the duration of CenturyLink's outage. In addition, TeleCommunication Systems' 911 systems that serve Tier 3 wireless service providers were fully operational and able to receive calls throughout the duration of CenturyLink's outage. However, during the following three time periods, due to the CenturyLink network outage, TeleCommunication Systems' data centers that provide Next Generation 911 services did not receive any 911 calls from callers served by North Central Texas 911 nor from callers in Washington. Simultaneously, its 911 systems did not receive calls that originated from its connected Tier 3 wireless service providers:

Dec. 27, 2018, 3:48 a.m. – Dec. 27, 2018, 4:16 a.m.

Dec. 27, 2018, 11:00 p.m. – Dec. 28, 2018, 6:26 a.m.

Dec. 28, 2018, 9:05 a.m. – Dec. 28, 2018, 9:57 a.m.

21. TeleCommunication Systems estimates that 8.4 million users were potentially affected and potentially could not make 911 calls during the times mentioned above. This includes 5.7 million potentially affected users in Washington, 1.6 million potentially affected users in north central Texas, and 1.1 million Tier 3 wireless customers in Washington and north central Texas.

22. TeleCommunication Systems initially learned of the network issue through its internal alarms and reports from PSAPs in Washington. TeleCommunication Systems' signal transfer points in Seattle and Phoenix sounded alarms. These alarms were triggered when TeleCommunication Systems experienced errors or loss of connectivity between its signal transfer points and SS7-signaling-provider-connected nodes. CenturyLink's outage affected enough of TeleCommunication Systems' SS7 links with its SS7 signaling provider, Transaction Network Services, Inc. (Transaction Network Services), to cause it not to receive 911 calls to then send to PSAPs.

23. TeleCommunication Systems was unable to reroute some calls around the CenturyLink outage. When it reached out to its SS7 signaling provider to investigate possible alternate routing strategies to reach the signal transfer points, Transaction Network Services stated that it was not able to provide any alternate routing.

24. On December 28, 2018, at 2:06 pm, TeleCommunication Systems confirmed that its above-referenced circuits from CenturyLink were stable and operational. TeleCommunication Systems continued to monitor the network for health and stability. On December 28, 2018, at 7:00 pm EST, TeleCommunication Systems performed a network evaluation, after which it declared the incident resolved.

### 2. Transaction Network Services, Inc.

25. Transaction Network Services provides SS7 service for TeleCommunication Systems and other small service providers. Transaction Network Services has paired signal transfer points in Las Vegas, Nevada and Los Angeles, California. TeleCommunication Systems connects to the Las Vegas and Los Angeles signal transfer points using four physically diverse links. CenturyLink provides TeleCommunication Systems and Transaction Network Services with transport for these links. As discussed above, CenturyLink's nodes intermittently became overloaded over the course of the outage.[34]

---

[33] SS7 is the network for traditional telecommunications upon which the exchange of control information associated with the setup and release of a telephone call on a telecommunications circuit occurs.

[34] *Supra* para. 13.

When one of those nodes that supported one of these four links became overloaded, that specific link went out of service. As the outage progressed, all four links were simultaneously down. In addition to the 911-related impacts described above, Transaction Network Services had SS7 connections fail where it relied on CenturyLink transport circuits, but such failures did not affect service due to alternative available routing.

### 3. General Dynamics Information Technology

26. General Dynamics Information Technology (General Dynamics) is Massachusetts's covered 911 service provider. As such, General Dynamics is responsible for delivering all 911 calls that originate in Massachusetts to the state's 305 PSAPs. General Dynamics relies on TeleCommunication Systems, which in turn relies on CenturyLink, to deliver 911 calls from Verizon, Verizon Wireless, and other service providers to the appropriate PSAPs. General Dynamics reported that the CenturyLink outage affected its ability as a Next Generation 911 (NG911) interconnection vendor to deliver 911 calls to PSAPs from service providers.

27. On December 28, 2018 between 12:30 a.m. and 7:39 p.m., General Dynamics estimates that TeleCommunication Systems was unable to receive signaling for approximately 800 calls to 911 initiating on several different service provider networks in transit to General Dynamics for processing. General Dynamics notified TeleCommunication Systems of these outage impacts around 1:00 a.m. on December 28. General Dynamics reports that it notified all Massachusetts PSAPs it served immediately after becoming aware of the outage. At 2:00 a.m., General Dynamics began regularly updating Massachusetts PSAPs on the outage and its effects. At 11:40 a.m. on December 28, the Massachusetts Emergency Management Agency, in coordination with the Massachusetts State 911 Department and General Dynamics, sent wireless emergency alerts to the public to use PSAPs' 10-digit numbers instead of 911.[35] General Dynamics-maintained NG911 infrastructure remained operational throughout the incident. It continued to process 911 calls as normal for service providers such as Comcast and AT&T Mobility.

### 4. West Safety Services

28. West Safety Services (West) relies upon CenturyLink's network to route some 911 calls to PSAPs. Specifically, CenturyLink's outage caused a service disruption in an element of West's network that provided access to selective routers that served 17 PSAPs in Texas and 7 PSAPs in Montana. This prevented West from successfully processing 911 calls destined for these selective routers. In Texas, the disruption began at 6:06 p.m. on December 27 and lasted until CenturyLink restored connectivity to the portion of the network upon which West relies at 11:07 a.m. on December 28. In Montana, the disruption began at 8:24 p.m. on December 27 and lasted until CenturyLink restored connectivity at 3:00 p.m. on December 28, 2018. The outage caused the failure of 75 calls to 911 in Texas and Montana. West states that it provided timely notification and updates to its affected PSAPs. West continued to process all other 911 calls in accordance with the originating service providers' pre-defined default routing plans. However, the affected PSAPs were unable to retrieve automatic number information (ANI), which provides the PSAP with the caller's phone number, and ALI, for any VoIP and wireless calls throughout the CenturyLink outage.

### 5. Verizon Wireless

29. Verizon Wireless uses CenturyLink to transport portions of its wireless network traffic.[36] The CenturyLink outage affected Verizon Wireless's network across several western states, including intermittent service problems in one county in Arizona, twelve counties in Montana, 21 counties in New

[35] Jonathan Ng, *Nationwide outage knocks out 911 call services in Massachusetts*, Boston Herald (Dec. 28, 2018), https://www.bostonherald.com/2018/12/28/nationwide-outage-knocks-out-911-call-services-in-massachusetts.

[36] *Nationwide internet outage affects CenturyLink customers*, Associated Press (Dec. 28, 2018), https://www.apnews.com/fc612a7689c74b98abd8bd4d1ed848c2.

Mexico,[37] and four counties in Wyoming.[38] One mobile switching center in New Mexico was isolated intermittently for 19 hours and 34 minutes beginning at 8:36 a.m. on December 27, with a total downtime of 10 hours and 48 minutes. In Arizona and New Mexico, this outage potentially affected 314,883 users of Verizon Wireless' network and resulted in 12,838,697 blocked calls (based on historical data). Once Verizon Wireless discovered that it was experiencing an outage, it tried to build a reroute in its network to mitigate the outage's effects. However, CenturyLink restored service before Verizon Wireless completed the reroute.

30. On December 27, the failures in CenturyLink's network caused a wireless network outage in Montana and Wyoming that potentially affected 92,613 users of Verizon Wireless's network and resulted in 1,922,586 blocked calls (based on historical data). In Montana, this event lasted for 24 hours and 19 minutes. In Wyoming, this event lasted for 13 hours and 16 minutes.

31. The CenturyLink outage also affected the ability of users of the Verizon Wireless network to access 911. In Texas, beginning at 12:06 a.m. on December 28, 37,045 potentially affected users were unable to reach 911 if their phones used Verizon Wireless's code division multiple access (CDMA) network that uses the affected CenturyLink network for transport due to the impact of the outage on a Verizon 911 service vendor. The outage lasted 12 hours and 1 minute. In Oregon, Verizon Wireless was unable to support ALI information for 12,673 potentially affected users on its CDMA network due to the impact of the outage on a Verizon 911 service vendor. This service degradation lasted for 29 hours and 26 minutes. However, the CenturyLink outage did not affect Verizon Wireless's ability to successfully process and transmit 911 calls on its LTE network, because the LTE network does not use the affected CenturyLink network for transport.

**6. Comcast**

32. Comcast relies on the affected CenturyLink network for transport to selective routers in Idaho and California. On December 27, 2018 at 6:06 a.m., Comcast network alarms indicated a loss of connectivity on some trunks used in Idaho and California for 911 call transport. Later that day, notifications from Comcast's third-party 911 vendors identified a potential disruption or degradation of 911 calling in multiple PSAPs in Alabama, Arizona, California, Colorado, Florida, Georgia, Iowa, Idaho, Illinois, Kansas, Maine, Montana, Minnesota, Oregon, Nebraska, New Mexico, Nevada, Pennsylvania, South Carolina, Tennessee, Utah, Virginia, and Washington. Comcast relies on CenturyLink-provided selective routers for 911 calls in each of these states. The outage potentially affected 3,552,495 of Comcast's VoIP customers for 49 hours and 32 minutes. Comcast VoIP customers may have experienced a fast-busy signal or diminished call quality if calls were transmitted over affected transport facilities. Upon discovery of the event, Comcast immediately notified potentially affected PSAPs.

33. CenturyLink provides transport for Comcast for its primary and secondary paths to selective routers in Idaho. Comcast also has a tertiary route, provided by a third party. CenturyLink's transport outage disrupted and degraded Comcast's ability to route 911 calls to PSAPs in Idaho over its primary and secondary paths, however, Comcast's backup tertiary route, using 10-digit phone numbers, remained operational. In addition, CenturyLink provides transport for Comcast's primary path to some selective routers in California. Comcast relies on a third party for secondary and tertiary routes. In the affected areas of California, 911 calls routed successfully to the redundant secondary route. ALI and ANI remained unaffected for VoIP calls in Idaho and California.

34. In the other states identified above, while 911 calls that would have relied on CenturyLink transport to reach PSAPs did not drop, some 911 calls may have been sent to fast-busy or

[37] Stephen Montoya, *CenturyLink, Verizon services disrupted*, Albuquerque Journal (Dec. 27, 2018), https://www.abqjournal.com/1261869/centurylink-verizon-see-widespread-outages-in-abq-area.html.

[38] *Nationwide internet outage affects CenturyLink customers*, Associated Press (Dec. 28, 2018), https://www.apnews.com/fc612a7689c74b98abd8bd4d1ed848c2.

encountered other call quality issues. Comcast Network Operations Center technicians performed test calls during the CenturyLink outage, which sometimes came back with a fast-busy signal. There was an increase in short-duration calls on Comcast's network during the CenturyLink outage, indicating that callers experiencing call quality issues hung up and redialed 911. Comcast reported that it notified its affected PSAPs and continued updating them over the course of the outage.

35. On December 28 at 5:36 p.m., CenturyLink notified Comcast that CenturyLink had removed the faulty module and undertaken additional actions to restore the network. Most services were restored by December 28 and all residual effects were resolved by December 29.

### 7. Effects on Other Providers

36. The CenturyLink outage also had smaller effects on other service providers. AT&T estimates that 1,778,250 users may have been affected. Some of the potential effects include dropped calls, voice service degradation, and callers receiving fast-busy signals when calling. TDS reported that 1,114 of its wireline users may have been affected. 911 call delivery was also affected for several service providers. Bluegrass Cellular, in Kentucky, reported that the outage potentially affected 911 call delivery for 195,384 wireless users. Cellcom, a Wisconsin-based wireless provider, notified the Commission that 53 calls to 911 were transmitted without ANI and ALI. Cox reported that the outage potentially affected 654,452 VoIP users. In Iowa, U.S. Cellular reported that the outage potentially affected ALI for 911 calls for 94,380 of its wireless users. None of the providers or PSAPs reported any harms to life or property due to the outage.

37. The table below summarizes the effects of the outage on all service providers, as discussed above.

| Provider | Provider Type | Number of Potentially Affected Users | Estimated Number of Affected Calls | Potential Effects |
|---|---|---|---|---|
| AT&T | Wireless Originating Service Provider | N/A | 1,778,250 | N/A |
| Bluegrass Cellular | Wireless Originating Service Provider | 195,384 | | 911 call delivery disruption |
| CenturyLink | Covered 911 Service Provider; Wireline Originating Service Provider; Transport Service Provider; | At least 3,750,000 | 12,100,108 | 911 call delivery disruption; ALI delivery failure; blocked calls; voice service degradation |
| Comcast | VoIP Service Provider | 3,553,495 | | 911 call delivery disruption |
| Cox | VoIP Service Provider | 654,452 | | |
| General Dynamics | Covered 911 Service Provider | 3,210,000 | 800 | 911 call delivery disruption |

| Provider | Provider Type | Number of Potentially Affected Users | Estimated Number of Affected Calls | Potential Effects |
|---|---|---|---|---|
| TDS | Wireline Originating Service Provider | 1,114 | | N/A |
| TeleCommunication Systems | Covered 911 Service Provider | 8,400,000 | | 911 call delivery disruption; ALI delivery failure |
| Transaction Network Services | SS7 Service Provider | N/A | N/A | |
| U.S. Cellular | Wireless Originating Service Provider | 94,380 | | ALI delivery failure |
| Verizon Wireless | Wireless Originating Service Provider | 407,496 | 14,272,966 | 911 call delivery disruption; blocked calls; voice service degradation |
| West | Covered 911 Service Provider | 499,387 | 75 | 911 call delivery disruption |

## V. CORRECTIVE ACTIONS BY CENTURYLINK AND INFINERA TO PREVENT RECURRENCE

38. After CenturyLink resolved the incident, it replaced the faulty switching module and shipped it to Infinera to perform a forensic analysis. Infinera's investigation is ongoing, but thus far Infinera engineers have been unable to replicate the malformed packet creation. CenturyLink and Infinera have taken additional steps to prevent a repeat of this particular outage. CenturyLink and Infinera reconfigured the nodes in the affected network by disabling the proprietary management channel. Infinera has disabled the channel on new nodes for CenturyLink's network and has updated the node's product manual to recommend disabling the channel if it is to remain unused. The service provider and vendor also established a network monitoring plan for network management events to detect similar events more quickly.[39] Currently, CenturyLink is in the process of updating its nodes' ethernet policer to reduce the chance of the transmission of a malformed packet in the future. The improved ethernet policer quickly identifies and terminates invalid packets, preventing propagation into the network. This work is expected to be complete in fall 2019.

39. CenturyLink also implemented improvements to its monitoring and audits of memory and processor utilization to enhance network engineers' visibility into issues of this type where processor utilization quickly escalates to unsustainable levels. Finally, CenturyLink used the outage as an opportunity to review and improve its customer notification process.

[39] Commission rules require covered 911 service providers to certify to diverse network monitoring. This requirement is unrelated to long-haul transport and the network monitoring discussed in this case. 47 CFR § 12.4(b).

## VI. NEXT STEPS

40. The Bureau plans to engage in stakeholder outreach and guidance regarding industry-accepted recommended network reliability best practices to protect against similar outages in the future. There are several best practices that could have prevented the outage, or at least mitigated its effects:

- System features that are not in use should be turned off or disabled.[40] In this case, the proprietary management channel was enabled by default so that it could be used if needed. While CenturyLink did not intend to use the feature, CenturyLink left it unconfigured and enabled. Leaving the channel enabled created a vulnerability in the network that, in this case, contributed to the outage by allowing malformed packets to be continually rebroadcast across the network.
- For unidentified failure modes, implementing filters can alleviate the impact of the failure. In this case, filters were designed to only mitigate specific risks. Thus, catch-all filters should be designed to only allow for expected traffic. In this event, the filter prevented transmission of packets 64 bytes or fewer over the proprietary management channel, regardless of packet content. Because other characteristics of the packet were not considered, the malformed packets were able to propagate.
- Network monitoring should include memory and processor utilization alarms that are regularly audited to ensure functionality and evaluated to improve early detection and calibration. As noted above, the malformed packets quickly overwhelmed the processing capacity of the nodes. This activity, however, did not trigger any processor utilization alarms indicating the rapidly diminishing ability of nodes to process traffic.
- Standard operating procedures for network repair should address cases where normal networking monitoring procedures are inoperable or otherwise unavailable. CenturyLink's network administrators were unable to connect to nodes remotely to locate and diagnose the outage or take corrective action because of node congestion. However, CenturyLink did execute a back-up plan that allowed for physical inspection of the nodes, allowing the company to discover the proximate cause of the outage (*i.e.*, the malformed packets) and to end the outage.

41. In keeping with past practice, the Bureau plans to release a Public Notice, based on its analysis of this and other recent outages, reminding companies of industry-accepted best practices, including those recommended by the Communications Security, Reliability and Interoperability Council, and their importance.[41] In addition, the Bureau will contact other major transport providers to discuss their network practices and will offer its assistance to smaller providers to help ensure that our nation's communications networks remain robust, reliable, and resilient.

---

[40] *See, e.g.*, Communications Security, Reliability and Interoperability Council, Best Practices 11-6-5170, 11-8-8000 (2011), https://opendata.fcc.gov/Public-Safety/CSRIC-Best-Practices/qb45-rw2t/data.

[41] *See, e.g.*, *Public Safety and Homeland Security Bureau Encourages Communications Service Providers to Follow Best Practices to Help Ensure Network Reliability*, Public Notice, 33 FCC Rcd 3776 (PSHSB 2018).